ABSTRACT

The increasing risk of website-based data security attacks is a concern for various parties, including PT. XYZ is a company that develops software for pharmacies and clinics which has helped more than 2500 pharmacies and clinics in more than 400 cities in Indonesia. The data stored therein includes sensitive information such as company data and customer information, which must be strictly guarded so that it does not fall into the wrong hands. The aim of this research is to identify vulnerabilities in PT's information system. XYZ and provides recommendations to improve security. The penetration testing method with OWASP Top 10 2021 is still very relevant and popular. The OWASP Top 10 contains the ten most critical web application security risks identified by security experts. In the Penetration Testing method, there are stages such as scope, reconnaissance, vulnerability detection, information analysis and planning, penetration testing, privilege escalation, result analysis, reporting, and clean-up. The success parameters of this research include the level of vulnerabilities identified, the success rate of attacks, and recommendations received to improve system security. With this research PT. XYZ can improve the security of its information systems and protect customer data more effectively. Based on the results of penetration testing with the OWASP Top 10 2021, several significant vulnerabilities were found, including problems with broken access control, cryptographic failures, SQL Injection, potential XSS through Referer headers, and security configuration issues such as lack of CSP headers and X-Frame-Options. Some components were also found to be vulnerable, such as outdated jQuery versions and CVEs in system components. In addition, issues related to authentication validation and failures in logging and monitoring were also identified. Recommendations for improvement include strengthening access control, configuring more secure cryptography, using parameterized queries to prevent SQL Injection, improving the configuration of security headers such as CSP and X-Frame-Options, updating system components, and improving authentication mechanisms and logging and monitoring systems to detect attack activity more effectively.

Keywords: Information system security, Owasp top 10, Penetration testing, PT XYZ , Website system security